[Use Case]

Third-Party Risk Management in Financial Services

Addressing Regulatory Pressure, Cyber Risk, and Operational Resilience

OVERVIEW

For hedge funds, asset managers, and other financial institutions, third-party vendors are essential, but they also represent one of the most significant and scrutinized risk vectors. Regulatory bodies like the SEC, FINRA, and NYDFS have made it clear: firms are accountable for the actions and security practices of their vendors. That means a weak third-party risk management (TPRM) program isn't just a vulnerability; it's a compliance failure waiting to happen.

In a sector where reputational damage, data breaches, or operational disruptions can lead to regulatory penalties and investor backlash, effective TPRM is no longer optional. It must be embedded across the vendor lifecycle and aligned with evolving regulatory requirements.

AN EFFECTIVE TPRM STRATEGY FOR FINANCIAL SERVICE PROVIDERS

An effective third-party risk management strategy should encompass the entire vendor lifecycle, from selection and onboarding to ongoing monitoring and eventual offboarding. The key objectives must include:

- **Risk Identification and Assessment:** Proactively identifying and assessing risks associated with each vendor and the vendor ecosystem as a whole, particularly risks related to cybersecurity, operational resilience, and compliance.
- **Continuous Monitoring:** Implementing continuous monitoring processes to ensure that vendors adhere to agreed-upon service levels, security standards, and regulatory requirements, and identifying vendors that do not live up to their assertions.
- **Incident Response and Recovery:** Ensuring that there are robust processes in place for responding to and recovering from vendor-related incidents, including data breaches and service disruptions.
- **Regulatory Compliance:** Confirming that vendor management processes align with regulatory requirements, such as those set by the SEC, FINRA, and GLBA, among others.
- **Cost Efficiency:** Optimizing the use of vendors through strategic management, avoiding unnecessary expenses, and ensuring value for money.

KEY THIRD PARTY REGULATORY CONCERNS FOR FINANCIAL FIRMS

1. SEC Regulation S-P (Updated 2024)

- **Scope:** This regulation focuses on safeguarding customer financial information, now extending these protections through third-party vendors.
- **Incident Response:** Firms must have incident response plans that include vendor breaches, ensuring customer notification within 30 days.
- **Vendor Due Diligence:** Firms must conduct thorough due diligence, reviewing vendor security measures such as SOC-2 reports and penetration test results.
- **Continuous Monitoring:** Ongoing oversight of vendor compliance is required to ensure data protection and regulatory.

2. FINRA Rules and Guidance

- **FINRA Rule 3110:** Requires firms to establish supervisory systems that include third-party vendors, ensuring compliance with securities laws.
- **FINRA Rule 4370:** Mandates the inclusion of third-party vendors in business continuity plans to ensure seamless operation during disruptions.
- **Cybersecurity Expectations:** FINRA emphasizes that firms must have cybersecurity programs that extend to their vendors, protecting customer information from breaches.

3. Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (Revised 2023)

- **Governance:** Requires the oversight of a qualified individual and regular board reporting on the security program.
- **Safeguards:** Expands requirements to include access controls, encryption, and multifactor authentication for vendor-managed data.
- **Testing:** Introduces requirements for continuous monitoring and penetration testing of vendor security measures.

4. NYDFS Cybersecurity Regulation (23 NYCRR 500)

- **Governance:** Involves the Board and CEO in cybersecurity risk management, including third-party vendors.
- **Access Controls:** Limits vendor access to only necessary data, requiring annual reviews.
- **Business Continuity:** Ensures that vendors are integrated into disaster recovery plans.

BEST PRACTICES FOR IMPLEMENTING A ROBUST TPRM PROGRAM

Third-party risk management is foundational to a financial services firm's risk strategy. Following these best practices helps ensure TPRM is not just a checkbox exercise but a deeply integrated part of the firm's overall risk management approach. By embedding these practices, firms can maintain control over vendor-related risks, uphold regulatory compliance, and ensure seamless operations even in the face of disruptions.

1. Comprehensive Vendor Due Diligence

- **Assess Vendor Risk:** Evaluate vendors based on their data access, cybersecurity controls, and historical compliance performance.
- **Contractual Obligations:** Ensure contracts with vendors clearly outline data protection responsibilities, incident response protocols, and compliance with regulatory requirements.

2. Continuous Monitoring and Testing

- **Regular Audits:** Conduct ongoing audits and "realtime" technical confirmation of vendor compliance with cybersecurity standards, focusing on data protection and operational resilience.
- **Penetration Testing:** Implement continuous monitoring and regular penetration tests of vendor systems to identify vulnerabilities.

3. Incident Response and Recovery

- **Integrated Incident Response:** Ensure that vendor-related incidents and vendor availability are covered in your firm's broader incident response plan.
- **Vendor Coordination:** Maintain clear communication channels with vendors for rapid response and recovery during cyber incidents.

4. Governance and Oversight

- **Board Involvement:** Engage the Board of Directors and/or Executive Committees in overseeing the firm's TPRM program, with regular updates on vendor-related risks and compliance status.
- **Policy Documentation:** Maintain documentation of TPRM policies and procedures, ensuring they align with industry standards and regulatory expectations.

5. Training and Awareness

- **Stakeholder Training:** Provide regular training on TPRM processes to all stakeholders, ensuring they understand their roles in managing vendor risks.
- **Cybersecurity Awareness:** Enhance training programs to cover the specific cybersecurity risks associated with third-party vendors, including the latest regulatory requirements.

SDG SOLUTION: ACTIONABLE TPRM GUIDANCE FOR FINANCIAL FIRMS

SDG helps financial institutions move from reactive vendor oversight to proactive risk governance—ensuring that third-party relationships are both secure and compliant.

Here's how we support your firm:

- **No-Cost TPRM Workshop for U.S.-Based Financial Firms**

  In a 2–4 hour session, SDG advisors will walk through your current TPRM program to identify foundational gaps across people, process, and technology. This workshop is complimentary for financial institutions with operations in the United States and is designed to quickly highlight exposure areas tied to regulatory expectations.

- **Comprehensive TPRM Maturity Assessment**

  A customizable engagement that benchmarks your TPRM program against regulatory obligations (e.g., SEC Regulation S-P, FINRA Rule 3110, GLBA, NYDFS 23 NYCRR 500) and industry best practices. The output includes:

  - A risk-aligned gap analysis
  - Maturity scoring by domain (e.g., due diligence, monitoring, incident response)
  - A tailored remediation roadmap across process, policy, and tooling
  - Recommendations for automation and vendor oversight tools to scale with your risk profile

CONCLUSION

Whether you're responding to recent regulatory updates or preparing for your next audit, SDG delivers the practical insight and compliance-driven structure needed to mature your TPRM program—fast.

Let us help you protect your firm, meet regulator expectations, and build a more resilient vendor ecosystem.

ABOUT US

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. To learn more visit www.sdgc.com or contact us at solutions@sdgc.com.

SDG
75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com

Contact Us: solutions@sdgc.com